PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 1/32	A1	(11) International Publication Number: WO 00/49797
		(43) International Publication Date: 24 August 2000 (24.08.00)

(21) International Application Number: PCT/US99/28290

(22) International Filing Date: 30 November 1999 (30.11.99)

(30) Priority Data:
09/251,093 16 February 1999 (16.02.99) US

(71) Applicant: PHILIPS ELECTRONICS NORTH AMERICA CORPORATION [US/US]; 1251 Avenue of the Americas, New York, NY 10020 (US).

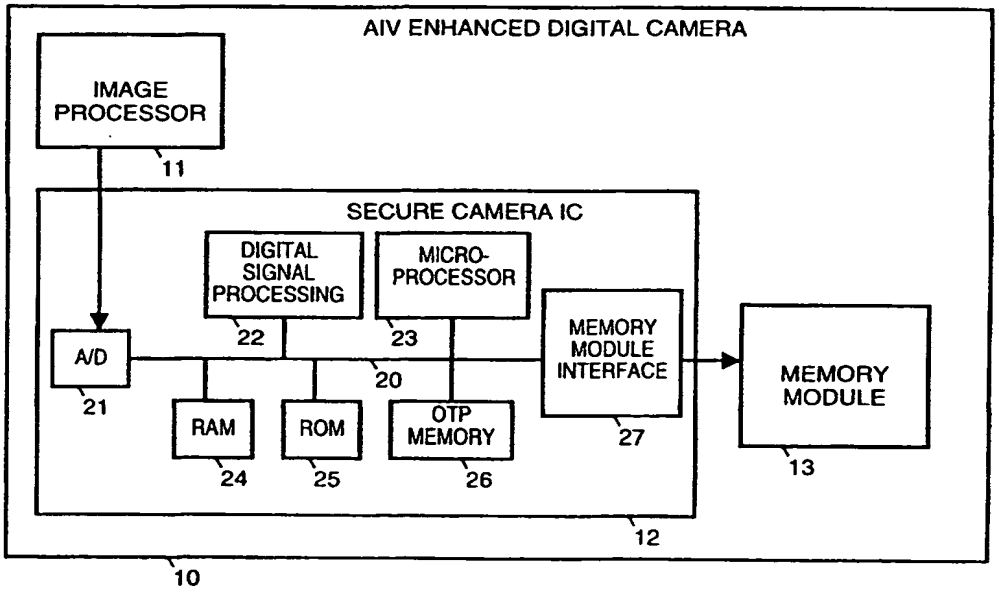
(72) Inventors: WALLACE, Joseph, Victor; 7091 S. Hazelton Lane, Tempe, AZ 85283 (US). BUER, Mark, Leonard; 1027 East Betsy Lane, Gilbert, AZ 85296 (US). KOWALSKI, John, Francis; 15038 South 25th Place, Phoenix, AZ 85048 (US).

(74) Agent: WELLER, Douglas, L.; 431 Magnolia Lane, Santa Clara, CA 95051-5637 (US).

(81) Designated States: CN, JP, KP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: AUTHENTICATION AND VERIFICATION WITHIN A DIGITAL CAMERA ARCHITECTURE



(57) Abstract

An enhanced digital camera includes a non-volatile memory in which is stored a security value used to produce digital signatures for photographs. A processor within the enhanced digital camera processes a photograph by hashing digital data for the photograph to produce a hash digest. The processor then performs a digital signature function using the security value in order to produce a digital signature for the photograph.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

AUTHENTICATION AND VERIFICATION WITHIN A DIGITAL CAMERA ARCHITECTURE

TECHNICAL FIELD

The present invention concerns digital cameras and pertains particularly to authentication and verification within a digital camera architecture.

BACKGROUND

As digital cameras become a widely used consumer item, there is a likelihood that photographs taken by digital cameras will increasingly be used for applications such as insurance claims and law enforcement. However, unlike previous photographic cameras, digital photography presents even the novice photographic enthusiast, using a standard personal computer, the means to "doctor" or manipulate photographs without detection. This is because digital cameras allow for photographs to be manipulated, modified and edited without degradation to the quality of the photograph. Consequently detection of such manipulations are not possible. This could present the opportunity for an unscrupulous individual to utilize digital photography to perform insurance fraud or to tamper with evidence used in a court of law.

SUMMARY OF THE INVENTION

In accordance with the preferred embodiment of the present invention, an enhanced digital camera includes a non-volatile memory in which is stored a security value used to produce digital signatures for photographs. A processor within the enhanced digital camera processes a

photograph by hashing digital data for the photograph to produce a hash digest. The processor then performs a digital signature function on the hash digest using the security value in order to produce a digital signature for the photograph.

In the preferred embodiment, the processor hashes a serial number for the camera and a date and time stamp along with the digital data for the photograph to produce the hash digest. The security value is, for example, a unique private key that is part of a private/public key pair. To increase security of the private key the non-volatile memory and the processor are within a secure integrated circuit and the processor generates the private/public key pair. The non-volatile memory is, for example, a one-time programmable memory. The public key is, for example, stored in a third party database and may be accessed (using the serial number for the enhanced digital camera) when it is necessary to authenticate a photograph taken by the enhanced digital camera.

The digital signature is stored with the digital data for the photograph. In order to authenticate the photograph, digital data for the photograph is hashed to produce a computed hash digest. For example, the serial number for the camera and the date and time stamp are hashed along with the digital data for the photograph. The public key for the enhanced digital camera is used to perform a digital signature function on the digital signature for the photograph in order to produce an extracted hash digest. The computed hash digest is compared with the extracted hash digest to determine whether the photograph is authentic and unaltered.

The authentication and integrity verification utilized by the enhanced digital camera architecture of the present invention provides the necessary functionality to authenticate photographs and to detect alterations.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a simplified block diagram of a digital camera architecture that incorporates authentication and verification in accordance with a preferred embodiment of the present invention.

Figure 2 illustrates an authentication and verification process within a digital camera in accordance with a preferred embodiment of the present invention.

Figure 3 illustrates a detection process used to detect modification of a digital picture and/or digital signature in accordance with a preferred embodiment of the present invention.

DISCLOSURE OF THE INVENTION

Figure 1 is a simplified block diagram of the architecture of an enhanced digital camera 10 that incorporates authentication and verification in order to provide the necessary functionality to protect digital photographic data from alterations. Digital camera 10, for example, can operate in an authentication and integrity verification (AIV) mode or in non-AIV mode. In AIV mode, enhanced digital camera 10 architecture authenticates and digitally signs each photograph as a picture is taken. This allows for detection of tampering with the original photograph. A hash function is used to protect the integrity of the original digital image and a digital signature function is used to protect the authenticity of the image.

The solution will not prevent tampering, rather it allows for detection of the tampering.

Enhanced digital camera 10 includes the typical functional blocks normally included within a digital camera. For example, enhanced digital camera 10 includes an image processor 11 and a memory module for storing pictures that have been taken.

A secure camera integrated circuit 12 contains other functional blocks of enhanced digital camera 10. These functional blocks are contained in a single integrated circuit, not only to reduce manufacturing cost, but also to provide a necessary level of security that does not allow a private key component to ever be exposed outside secure camera integrated circuit 12.

The functional components included within secure camera integrated circuit 12 are an analog-to-digital (A/D) converter block 21, a digital signal processing block 23, random access memory (RAM) 24, read-only memory (ROM) 25 and a memory module interface 27.

In addition, secure camera integrated circuit 12 includes a one-time programmable (OTP) memory 26. One-time programmable memory 26 is a secure memory that stores the security value of the digital camera. Alternative to a one-time programmable memory, memory 26 could be manufactured from flash memory, programmable read-only memory (PROM), EEPROM, or any other memory that can permanently and securely store the security value of enhanced digital camera 10.

The security value of enhanced digital camera 10 is, for example, a unique public/private key pair. Alternatively, the security value of the digital camera is any unique security value that can be used to produce a digital signature.

For example, microprocessor 23 generates a public/private key pair at the time of manufacture of enhanced digital camera 10. Microprocessor 23 programs the generated public/private key pair into OTP memory 26. The public key component of the public/private key is then sent out of secure camera integrated circuit 12 and enhanced digital camera 10. The public key is then recorded, along with the serial number, for example, by a secure third party (Certificate Authority), for purposes of later authenticating and verifying the integrity of a photograph. For example, the secure third party could be a company that is in the business of issuing digital certificates for individuals and corporations.

Figure 2 illustrates an authentication and verification process that is utilized by enhanced digital camera 10 in accordance with a preferred embodiment of the present invention. When a photograph is snapped, the resulting digital data 31 is stored in RAM 24. A date and time stamp 41, generated by a real-time clock 32, is prepended to digital data 31. Also prepended to digital data 31 is a camera serial number 42 of enhanced digital camera 10. A hash function 34 is used to hash together digital data 31, date and time stamp 41 and camera serial number 42 in order to generate a hash digest 35. A digital signature function 37 digitally signs hash digest 35 with a unique private key 36 to produce a digital signature 44. Unique private key 37 is a private key which is used only for enhanced digital camera 10. Digital signature 44 is appended to digital data 31. The entire structure for the photograph, including data/time stamp 41, camera serial number 42, digital data 31 and digital signature 44, is stored in memory module 13.

The stored structure for the photograph allows the photograph to be authenticated. In effect, a digital fingerprint of the photograph has been created as the photograph is taken. This allows any changes to the picture to be detected.

The preferred embodiment of the present invention resists attack by those trying to circumvent the protection system. The two most obvious ways to attack the protection system would be to modify the photograph (digital data 31) and return it to memory module 13 or to modify the photograph (digital data 31) and digital signature 44, so the two match, and return the result to memory module 13. Either of these attacks, however, can be protected utilizing the preferred embodiment of the present invention.

Figure 3 illustrates a detection process used to detect when the photograph (digital data 31) has been modified and returned to memory module 13 or when the photograph (digital data 31) and digital signature 44 have both been modified and then returned to memory module 13.

A secure database 60 is used to store public keys for enhanced digital cameras. For example, database 60 is a third party database used to archive the camera serial numbers and associated public keys. As show in Figure 3, each of representative entries 61, 62, 63 and 64 includes a camera serial number and an associated public key.

In order to detect whether a digital data 53 within a structure 50 has been modified, a hash function 71 is used to hash together digital data 53, a date and time stamp 51 and a camera serial number 52 in order to generate a computed hash digest 72. Camera serial number 52 is used to access from database 60 a unique public key 73 for the enhanced digital camera. A digital signature function 74 uses unique public key 73 to extract from digital

signature 50 an extracted hash digest 75. A compare function 76 compares computed hash digest 72 with extracted hash digest 75 and an output 77 indicates whether there is a match (i.e., the photograph is authentic and unaltered) or there is not a match (i.e., the photograph is not authentic or has been altered).

The detection process in Figure 3 detects both the case where a photograph has been modified and returned to a memory module and the case where a photograph and digital signature have been modified and both returned to memory module 13. Modifying the photograph (but not the signature) and returning it to the memory module would result in a mismatch of the hash value of the new picture and the hash value stored in the signature. Modifying both the photograph and the signature would also result in a mismatch of the computed hash value and the hash value stored in the signature. Even though the hash value stored in the signature was properly computed, unless the hash value is signed with the correct private key, it will be detected as an altered photograph. Thus, someone attempting to sign a photograph with a non-registered public/private key pair could be detected.

While the present invention provides significant protection, there are possible ways an attempt could be made to circumvent the protection system. For example, an attempt could be made to extract the private key from a registered camera via a physical attack. The extracted private key could then be used to sign the hash value of a modified photograph. In the event this type of tampering is suspected, it may be necessary to examine the enhanced digital camera for signs of tampering to determine whether a physical attack has occurred. Also precautions can be taken when

designing secure camera IC 12 to assure that the private key would be very difficult to access by an attacker. The strength and integrity of the system is predicated on the ability to store data (i.e., a private key) internal to the camera in a secure manner. The most effective way to do this, as described above, is to utilize a one-time programmable memory that is fully integrated into a single chip architecture in the enhanced digital camera. In this way, it is never necessary for the private key information to be sent outside the secure integrated circuit and increasing the ability to protect the integrity of photographs.

Another potential attack on the integrity of the system would be for an attacker to access database 60 in order to insert a bogus public key. Photographs could then be "authenticated" with a bogus private key related to the bogus public key. However, inserting a bogus public key into a secured, third-party database could be difficult to achieve without detection. Databases used for securing digital signatures are typically digitally signed by the third party, adding an additional layer of security. Providing similar safeguards for database 60 would provide significant protection to the embodiments of the present invention.

The foregoing discussion discloses and describes merely exemplary methods and embodiments of the present invention. As will be understood by those familiar with the art, the invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. Accordingly, the disclosure of the present invention is intended to be illustrative, but not limiting, of the scope of the invention, which is set forth in the following claims.

CLAIMS

We Claim:

1. A method for protecting a photograph taken by a digital camera comprising the following steps:

(a) hashing digital data for the photograph to produce a hash digest; and,

(b) performing a digital signature function on the hash digest using a security value in order to produce a digital signature for the photograph.

2. A method as in claim 1 additionally comprising the following step:

(c) storing the digital signature with the digital data for the photograph.

3. A method as in claim 1 wherein step (a) includes hashing a serial number for the camera along with the digital data for the photograph to produce the hash digest.

4. A method as in claim 1 wherein step (a) includes hashing a serial number for the camera and a date and time stamp along with the digital data for the photograph to produce the hash digest.

5. A method as in claim 1 wherein in step (b) the security value is a unique private key which is part of a private/public key pair.

6. A method as in claim 1 wherein step (a) and step (b) are both performed within a secure integrated circuit.

7. A method for authenticating a photograph taken by a digital camera comprising the following steps:

(a) hashing digital data for the photograph to produce a computed hash digest;

(b) accessing a security value for the digital camera;

(c) using the security value for the digital camera to perform a digital signature function on a digital signature for the photograph in order to produce an extracted hash digest; and,

(d) comparing the computed hash digest with the extracted hash digest to determine whether the photograph is authentic.

8. A method as in claim 7 wherein in step (c) the digital signature is stored with digital data for the photograph.

9. A method as in claim 7 wherein step (a) includes hashing a serial number for the camera along with the digital data for the photograph to produce the computed hash digest.

10. A method as in claim 7 wherein step (a) includes hashing a serial number for the camera and a date and time stamp along with the digital data for the photograph to produce the computed hash digest.

11. A method as in claim 7 wherein in step (b) the security value is a public key which is part of a private/public key pair.

12. An enhanced digital camera, comprising:

a non-volatile memory in which is stored a security value used to produce digital signatures for photographs; and,

a processor, the processor processing a photograph by hashing digital data for the photograph to produce a hash digest and the processor performing a digital signature function on the hash digest using the security value in order to produce a digital signature for the photograph.

13. An enhanced digital camera as in claim 12 wherein the processor stores the digital signature with the digital data for the photograph.

14. An enhanced digital camera as in claim 12 wherein when the processor hashes the digital data for the photograph, the processor hashes a serial number for the camera along with the digital data for the photograph to produce the hash digest.

15. An enhanced digital camera as in claim 12 wherein when the processor hashes the digital data for the photograph, the processor hashes a serial number for the camera and a date and time stamp along with the digital data for the photograph to produce the hash digest.

16. An enhanced digital camera as in claim 12 wherein the security value is a unique private key which is part of a private/public key pair.

17. An enhanced digital camera as in claim 12 wherein the non-volatile memory and the processor are within a secure integrated circuit.

18. An enhanced digital camera as in claim 12 wherein the non-volatile memory is a one-time programmable memory.

19. An enhanced digital camera as in claim 12 wherein the processor generates the security value.

20. An enhanced digital camera as in claim 12 wherein the security value is a unique private key which is part of a private/public key pair which is generated by the processor.

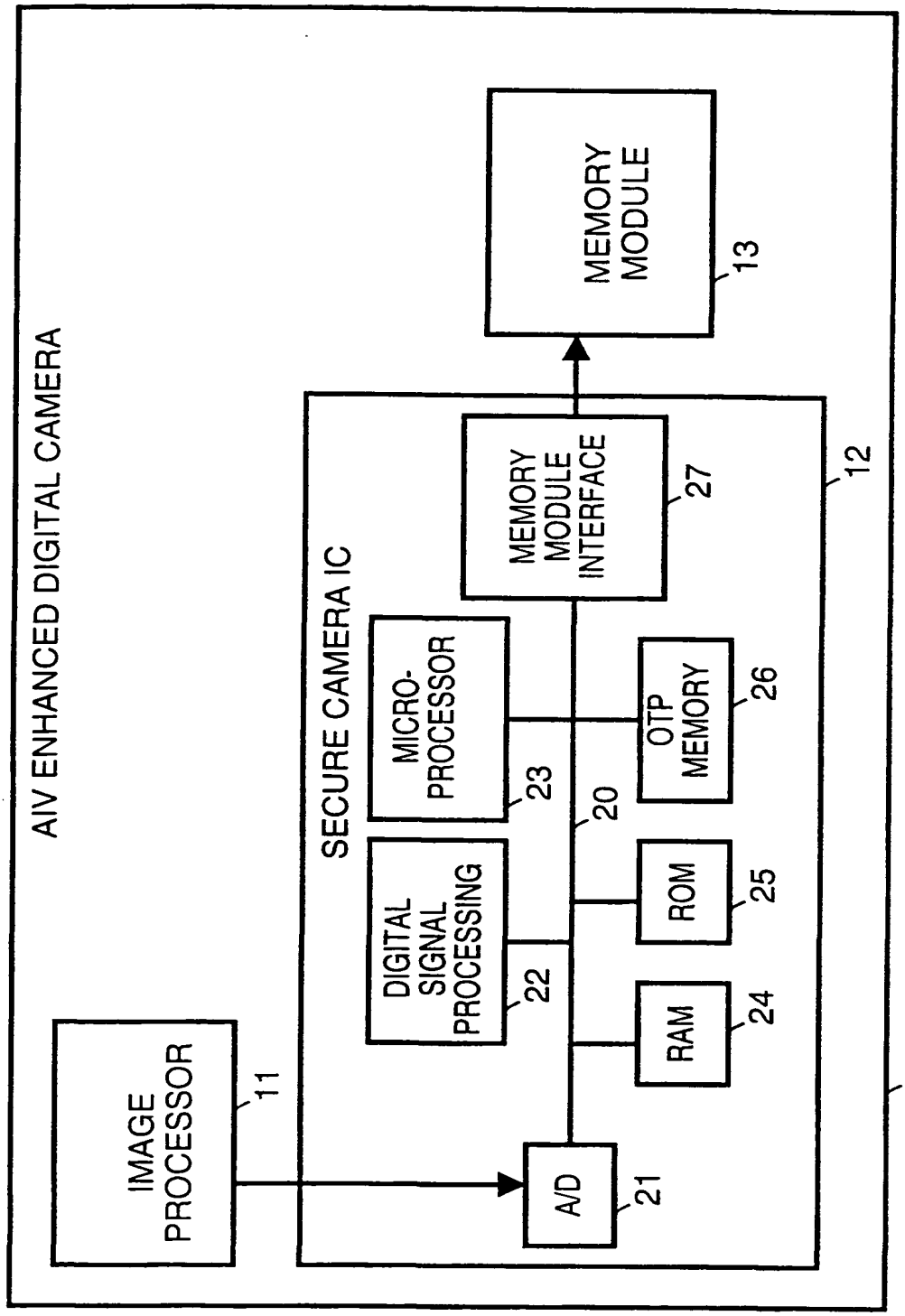

AIV ENHANCED DIGITAL CAMERA
SECURE CAMERA IC
IMAGE PROCESSOR
11
A/D
21
DIGITAL SIGNAL PROCESSING
22
MICRO-PROCESSOR
23
RAM
24
ROM
25
OTP MEMORY
26
MEMORY MODULE INTERFACE
27
MEMORY MODULE
13
20
12
10

FIGURE 1

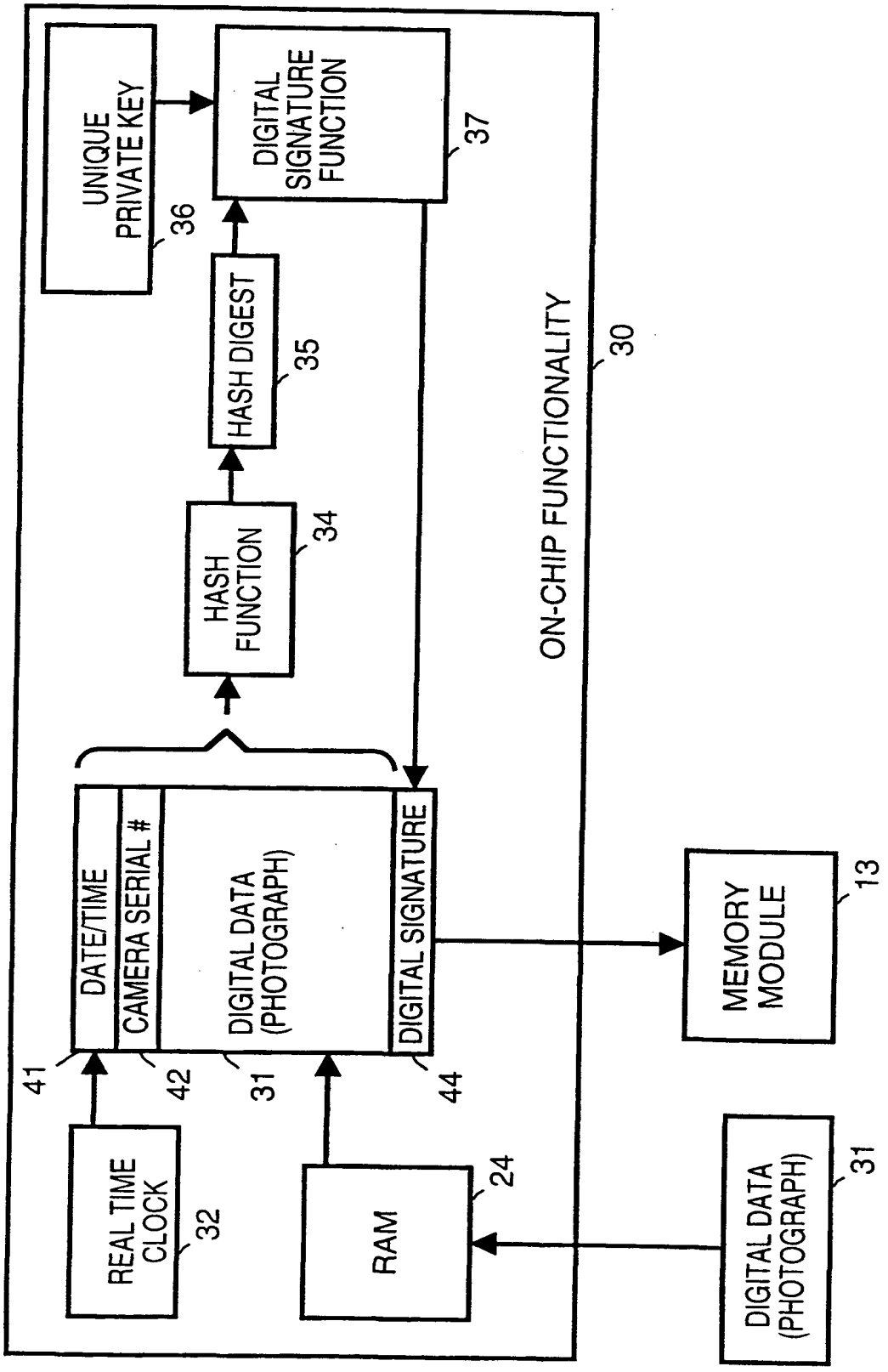

ON-CHIP FUNCTIONALITY
30
UNIQUE PRIVATE KEY
36
DIGITAL SIGNATURE FUNCTION
37
HASH DIGEST
35
HASH FUNCTION
34
DATE/TIME
CAMERA SERIAL #
DIGITAL DATA (PHOTOGRAPH)
DIGITAL SIGNATURE
41
42
31
44
REAL TIME CLOCK
32
RAM
24
MEMORY MODULE
13
DIGITAL DATA (PHOTOGRAPH)
31

FIGURE 2

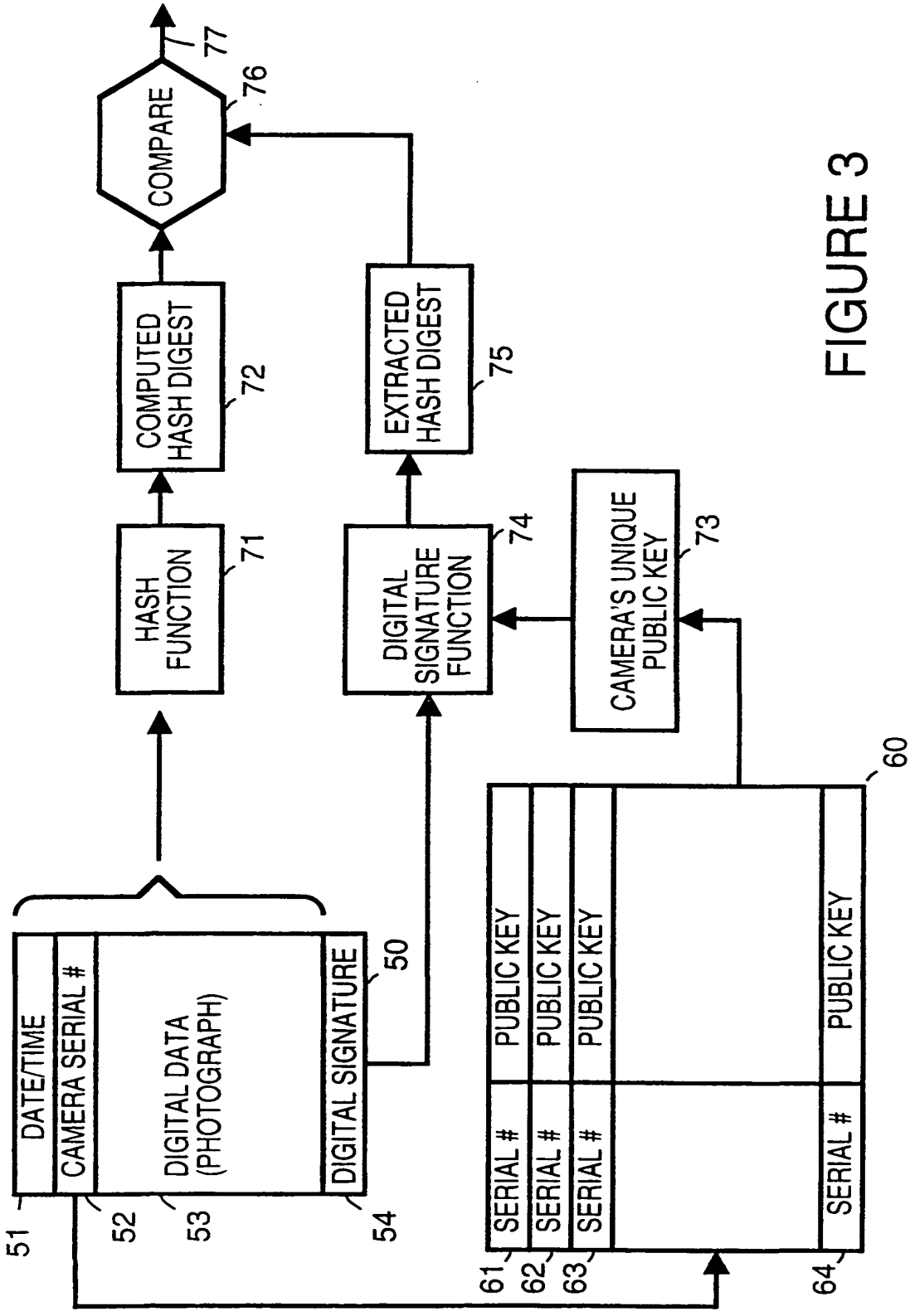


FIGURE 3

INTERNATIONAL SEARCH REPORT

Inte Jonal Application No
PCT/US 99/28290

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 845 758 A (IBM) 3 June 1998 (1998-06-03) abstract column 1, line 37 -column 2, line 43 column 4, line 43 - line 51 column 6, line 20 - line 32	1-20
X	US 5 499 294 A (FRIEDMAN GARY L) 12 March 1996 (1996-03-12) abstract column 1, line 15 - line 20 column 2, line 18 - line 23 column 4, line 19 - line 63 column 5, line 49 -column 6, line 43	1-20

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 April 2000	02/05/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Stoffers, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte. ional Application No
PCT/US 99/28290

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 801 856 A (RABBANI MAJID ET AL) 1 September 1998 (1998-09-01) abstract; figures 3,4 column 2, line 11 - line 15 column 2, line 41 - line 65 column 3, line 38 - line 48 claims 1,3	1-3,5-7, 11
P,X	US 5 898 779 A (RABBANI MAJID ET AL) 27 April 1999 (1999-04-27) abstract column 2, line 36 - line 43	1,2,5-8, 11-13, 16-18

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte. ional Application No
PCT/US 99/28290

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0845758 A	03-06-1998	JP 10164549 A	19-06-1998
		CA 2222346 A	28-05-1998
		CN 1184294 A	10-06-1998
		US 6005936 A	21-12-1999
US 5499294 A	12-03-1996	NONE	
US 5801856 A	01-09-1998	NONE	
US 5898779 A	27-04-1999	NONE	